REMARKS

In the Office Action, the Examiner rejected Claims 1-5, 7-9, 11-13, 15 and 16, which are all of the pending claims, under 35 U.S.C. 103 as being unpatentable over the prior art and under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. With respect to the rejection of the claims over the prior art, Claims 1, 2, 15 and 16 were rejected as being unpatentable over U.S. Patent 5,878,138 (Yacobi) in view of U.S. Patent 6,298,153 (Oishi); and Claims 3-5, 7-9 and 11-13 were rejected as being unpatentable over U.S. Patent 6,675,153 (Cook, et al.) n view of Oishi.

For the reasons discussed below, the rejections of the claims under 35 U.S.C. 103 and 112 are both respectfully traversed. The Examiner is, accordingly, asked to reconsider and to withdraw these rejections of Claims 1-5, 7-9, 11-13, 15 and 16, and to allow these claims. Also, this opportunity is being taken to amend independent Claims 1, 3, 7 and 11 to better define the subject matters of these claims. Claim 15 is being amended to keep the language of this claim consistent with the language of Claim 1, from which Claim 15 depends.

The present invention, generally, relates to methods and systems to create and manage digital cash. With a preferred embodiment of the invention, a customer sends a request for digital cash to a bank, along with a public key of an encryption scheme. The bank signs the cash using a secret key of a digital signature scheme, and encrypts the signature by using the public key provided by the customer. The bank also encrypts an unsigned copy of the cash.

The bank sends back to the customer a copy of the encrypted signed cash and a copy of the encrypted unsigned cash. The customer then decrypts both the signed and unsigned copies of the cash using the private key of the encryption scheme, and can then use the cash for payment to a third party. This third party, using the copy of the cash signed by the bank,

is then able to ask the bank to confirm the validity of the digital cash, and once that validity is confirmed, this third party can redeem the digital cash for payment.

In rejecting the claims under 35 U.S.C. 1 12, the Examiner argued that the limitation "both an encrypted copy of the signed coin and an encrypted copy of the unsigned coin" Is not enabled by the specification.

This aspect of the invention is explained at several places in the specification. For example, from page 9, line 25 to page 10, line 20, it is specifically explained how to generate these two copies. As explained there, each unit (Unit) is signed by the secure cryptography generator. The signature is then encrypted by using the customer's public encryption scheme. In addition, as mentioned on page 10, line 4, the secure cryptography generator also encrypts the unsigned unit (Unit). It is explained later on page 10, that, among other values, the encrypted signed unit (Encr2(Sign1(Unit))) and the encrypted unsigned unit (Encr2(Unit)) are both sent first to the computer system of the bank, and then to the customer C.

In light of the above-discussion, it is believed that the specification fully enables and explains how the encrypted copy of the signed coin and the encrypted copy of the unsigned coin are formed and used in the present invention. Applicants thus respectfully ask that the Examiner reconsider and withdraw the rejection of Claims 1-5, 7-9, 11-13, 15 and 16 under 35 U.S.C. 112.

Moreover, it is the use of this pair of copies of the coin – that is, encrypted copies of the signed and unsigned coin – that distinguish the claims of the application from the prior art. More specifically, with these two copies, a third party can readily determine the amount of the coin without decoding the signed copy, and this third party can, by using the signed copy, confirm that amount with the bank.

The references of record do not disclose or suggest this feature of the instant invention.

Yacobi, for example, describes procedures for using electronic cash or electronic assets. In one specific procedure discussed in Yacobi, a tamper resistant electronic wallet is used to store the asset. This wallet is intended to detect fraud and to eliminate further fraud before the criminal has had an opportunity to profit from the fraud. Yacobi also discloses, from column 12, line 50 to column 15, line 10, a blind re-certification process; however, this process uses a blind signature, as specifically discussed in column 12, lines 50-64.

Cook, et al, like Yacobi, discloses a procedure for using electronic cash or electronic assets. Cook, et al, more particularly, describes a system for authorizing electronic transactions between a consumer and a merchant. One objective of this system is to keep the consumer anonymous to the merchant, not to keep the consumer anonymous from the issuer or certifying authority.

Oishi discloses several digital signature procedures, including the use of an anonymous public key certificate. As explained in the present application, non-homomorphic signature schemes are, per se, known. Oishi does not relate to digital cash, and does not provide any suggestion or guidance as to how to use effectively the disclosed cryptographic method in a digital cash system. In particular, Oishi clearly does not address the same specific problem that is effectively addressed by the present invention – to provide secure digital cash that can be used by a customer in a conventional manner while still maintaining the customer's identity anonymous to the bank.

In the Office Action, the Examiner cited specific portions of Oishi and Cook, et al. as allegedly disclosing the feature of sending back to a user encrypted copies of both a signed coin and an unsigned coin. For instance, the Examiner referred to column 11, lines 48-54 of

Oishi. This portion of Oishi describes a certificate publisher terminal device that has a public key generating unit and a signature-generating unit. There is no teaching of encrypting both signed and unsigned copies of a coin, yet alone of using those encrypted copies in the manner in which they are used in the present invention.

The Examiner also specifically referred to column 16, lines 41-52 of Cook, et al. This portion of Cook, et al simply describes encrypting a member and merchant information response, and sending that encrypted information to a charge slip application. Here too, there is no teaching of encrypting signed and unsigned copies of a coin and using those encrypted copies as they are used in the instant invention.

Independent Claims 1, 3, 7 and 11 are being amended to describe the above-discussed feature of this invention in a more positive manner. More specifically, Claim 1, as amended herein describes the feature of forming an encrypted copy of the signed coin and an encrypted copy of the unsigned coin using a public key of a given encryption scheme, sending both of those copies of the coin back to the user. Claim 1 also describes the feature that the user has the private key of the given encryption scheme and can use that key to decrypt both the signed and unsigned copies of the coin.

Claims 3 and 11, as amended herein, describe the feature that the encrypted signed unit and the encrypted unsigned unit are encrypted using a public key of a given public key/private key encryption scheme, that both of these units are transmitted back to the customer who then decrypts both of these units using the private key of the encryption scheme. Claim 7 is directed to a system for creating and managing electronic cash and describes analogous apparatus features.

The other references of record have been reviewed, and these other references, whether considered individually or in combination, are not believed to be any more relevant than Yacobi, Oishi and Cook, et al. In particular, these other references also do not suggest or disclose the use of two copies of the encrypted cask in the above-described manner.

Because of the above-discussed differences between Claims 1, 3, 7 and 11 and the prior art, and because of the advantages associated with those differences, these claims patentably distinguish over the prior art and are allowable. Claim 2 is dependent from, and is allowable with, Claim 1; and Claims 4, 5, 15 and 16 are dependent from Claim 3 and are allowable therewith. Similarly, Claims 8 and 9 are dependent from Claim 7 and are allowable therewith; and Claims 12 and 13 are dependent from, and are allowable with, Claim 11.

For the reasons discussed above, the Examiner is asked to reconsider and to withdraw the rejections of Claims 1-5, 7-9 and 11-13, 15 and 16 under 35 U.S.C. 103 and 112, and to allow these claims. If the Examiner believes that a telephone conference with Applicants' Attorneys would be advantageous to the disposition of this case, the Examiner is asked to telephone the undersigned.

Respectfully submitted,

John S Sensny

John S. Sensny
Registration No. 28,757
Attorney for Applicants

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza - Suite 300
Garden City, New York 11530
(516) 742-4343

JSS:jy